What is claimed is:

1	 A system for providing telephonic content security service in a
2	wireless network environment, comprising:
3	a plurality of wireless devices interfacing over a network providing
4	wireless telephonic services through a layered service architecture;
5	a provisioning framework provisioning content security services to the
6	wireless devices via the layered service architecture, each content security service
7	delivered through applications executing in a user layer on each wireless device,
8	comprising:
9	a network operations center supervising the provisioning of the
10	content security services to each wireless device and maintaining a master catalog
11	of the applications and configured wireless devices list; and
12	a configuration client managing a configuration of each wireless
13	device by consulting the master catalog and the configured wireless devices list
14	and downloading the applications to each wireless device; and
15	each wireless device delivering the content security services as
16	functionality provided through execution of the applications.
1	2. A system according to Claim 1, further comprising:
1	2. A system according to Claim 1, further comprising:a status daemon periodically pushing operational data from each wireless
2	
3	device to the network operations center.
1	3. A system according to Claim 2, further comprising:
2	a status daemon pulling operational data from each wireless device to the
3	network operations center on-demand.
_	A A A A A A A Claim 2 further comprising:
1	4. A system according to Claim 2, further comprising:
2	a reporting module creating at least one of an informational report and a
3	statistics report from the operational data.
1	5. A system according to Claim 2, further comprising:

2	a reporting module generating an alert from the operational data upon
3	detecting a faulty wireless device.
1	6. A system according to Claim 1, wherein the applications further
2	comprise support files, further comprising:
3	a configuration client providing at least one of updates to the applications
4	and modifications to the support files to the wireless devices.
1	7. A system according to Claim 6, wherein the updates and the
2	modifications are periodically downloaded from the network operations center.
1	8. A system according to Claim 6, wherein the updates and the
2	modifications are downloaded from the network operations center on-demand.
1	9. A system according to Claim 1, further comprising:
2	an application repository maintained on a remote component server
3	storing the applications under control of the network operations center.
1	10. A system according to Claim 1, further comprising:
2	a local application repository maintained on a local component server
3	storing the applications under control of the network operations center.
1	11. A system according to Claim 1, wherein the content security
2	service comprises antivirus scanning and the application comprises an antivirus
3	scanner.
1	12. A method for providing telephonic content security service in a
2	wireless network environment, comprising:
3	interfacing to a plurality of wireless devices over a network providing
4	wireless telephonic services through a layered service architecture;
5	provisioning content security services to the wireless devices via the
6	layered service architecture, each content security service delivered through
7	applications executing in a user layer on each wireless device, comprising:

8	supervising the provisioning of the content security services to
9	each wireless device from a network operations center at which are maintained a
10	master catalog of the applications and configured wireless devices list; and
11	managing a configuration of each wireless device from a
12	configuration client by consulting the master catalog and the configured wireless
13	devices list and downloading the applications to each wireless device; and
14	delivering the content security services as functionality provided through
15	execution of the applications on each wireless device.
1	13. A method according to Claim 12, further comprising:
2	periodically pushing operational data from each wireless device to the
3	network operations center.
1	14. A method according to Claim 13, further comprising:
2	pulling operational data from each wireless device to the network
3	operations center on-demand.
1	15. A method according to Claim 13, further comprising:
2	creating at least one of an informational report and a statistics report from
3	the operational data.
1	16. A method according to Claim 13, further comprising:
2	generating an alert from the operational data upon detecting a faulty
3	wireless device.
1	17. A method according to Claim 12, wherein the applications further
2	comprise support files, further comprising:
3	providing at least one of updates to the applications and modifications to
4	the support files to the wireless devices.
1	18. A method according to Claim 17, further comprising:
2	periodically downloading the updates and the modifications from the

network operations center.

3

1	19. A method according to Claim 17, further comprising:
2	downloading the updates and the modifications from the network
3	operations center on-demand.
1	20. A method according to Claim 12, further comprising:
1	· ·
2	maintaining an application repository on a remote component server
3	storing the applications under control of the network operations center.
1	21. A method according to Claim 12, further comprising:
2	maintaining a local application repository on a local component server
3	storing the applications under control of the network operations center.
1	22. A method according to Claim 12, wherein the content security
2	service comprises antivirus scanning and the application comprises an antivirus
3	scanner.
3	Scamer.
1	23. A computer-readable storage medium holding code for performing
2	the method according to Claims 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, or 22.
1	24. A system for provisioning a plurality of wireless devices in a
2	closed content security service loop framework, comprising:
3	a wireless network environment comprising a plurality of wireless devices
4	each providing wireless telephonic services;
5	a centralized database comprising catalogs of configuration information
6	for the wireless devices;
7	a configuration client determining the content security service components
8	required for content security service delivery from the configuration information
9	catalogs and providing the content security service components to each wireless
10	device for configuration and execution; and
11	a network operations center delivering content security services to each
12	wireless device through the content security service components being executed
13	thereon, and periodically receiving a status report from each wireless device

14	providing status information comprising machine-specific data and application-
15	specific information.
1	25. A system according to Claim 24, further comprising:
2	an applet executing on the configuration client broadcasting a query
3	message to one or more unconfigured wireless devices and receiving
4	configuration requests from each unconfigured wireless device.
1	26. A system according to Claim 24, further comprising:
2	a catalog server generating a catalog of out-of-date content security
3	service components on each wireless device.
1	27. A system according to Claim 24, further comprising:
2	an applet executing on the configuration client updating the out-of-date
3	content security service components on each wireless device.
1	28. A system according to Claim 24, further comprising:
2	a component server staging the content security service components.
1	29. A system according to Claim 28, further comprising:
2	a network operations center storing the staged content security service
3	components.
1	30. A system according to Claim 28, further comprising:
2	at least one of a remote component server and a local component server
3	storing the staged content security service components.
1	31. A system according to Claim 24, further comprising:
2	a Web browser executing an applet on the configuration client to manage
3	the configuration of the content security service components on each wireless
-4	device.
1	32. A method for provisioning a plurality of wireless devices in a
2	closed content security service loop framework, comprising:

3	providing a wireless network environment comprising a plurality of
4	wireless devices, each providing wireless telephonic services;
5	maintaining a centralized database comprising catalogs of configuration
6	information for the wireless devices;
7	determining the content security service components required for content
8	security service delivery from the configuration information catalogs and
9	providing the content security service components to each wireless device for
10	configuration and execution;
11	delivering content security services to each wireless device through the
12	content security service components being executed thereon; and
13	periodically receiving a status report from each wireless device providing
14	status information comprising machine-specific data and application-specific
15	information.
1	33. A method according to Claim 32, further comprising:
2	broadcasting a query message to one or more unconfigured wireless
3	devices; and
4	receiving configuration requests from each unconfigured wireless device.
7	receiving comiguration requests from each uncomigured wireless device.
1	34. A method according to Claim 32, further comprising:
2	generating a catalog of out-of-date content security service components on
3	each wireless device.
1	35. A method according to Claim 32, further comprising:
2	updating the out-of-date content security service components on each
3	wireless device.
J	WITCHOSS device.
1	36. A method according to Claim 32, further comprising:
2	staging the content security service components on a component server.
1	37. A method according to Claim 36, further comprising:
2	storing the staged content security service components on a network
3	operations center.
J	operations conter.

ī	38. A memod according to Claim 30, further comprising.
2	storing the staged content security service components on at least one of a
3	remote component server and a local component server.
1	39. A method according to Claim 32, further comprising:
2	executing an applet configuration client on a Web browser to manage the
3	configuration of the content security service components on each wireless device.
1	40. A computer-readable storage medium holding code for performing
2	the method according to Claims 32, 33, 34, 35, 36, 37, 38, or 39.